A generalization of sumsets modulo a prime

Francesco Monopoli[1]

Dipartimento di Matematica, Università degli Studi di Milano
via Saldini 50, Milano
I-20133 Italy

Abstract

Let A be a set in an abelian group G. For integers $h, r \geq 1$ the generalized h-fold sumset, denoted by $h^{(r)}A$, is the set of sums of h elements of A, where each element appears in the sum at most r times. If $G = \mathbb{Z}$ lower bounds for $|h^{(r)}A|$ are known, as well as the structure of the sets of integers for which $|h^{(r)}A|$ is minimal. In this paper we generalize this result by giving a lower bound for $|h^{(r)}A|$ when $G = \mathbb{Z}/p\mathbb{Z}$ for a prime p, and show new proofs for the direct and inverse problems in $\mathbb{Z}$.

Keywords: Sumsets modulo a prime, Erdős-Heilbronn conjecture

2010 MSC: Primary: 11B13, Secondary: 11P70.

1. Introduction

Let $A = \{a_1, \ldots, a_k\}$ be a set of k elements in an abelian group G.

Given integers $h, r \geq 1$ define

$$h^{(r)}A = \left\{ \sum_{i=1}^{k} r_i a_i : 0 \leq r_i \leq r \text{ for } i = 1, \ldots, k \text{ and } \sum_{i=1}^{k} r_i = h \right\}.$$

Note that the usual sumsets

$$hA = \{a_{j_1} + \cdots + a_{j_h} : a_{j_i} \in A \ \forall i = 1, \ldots, h\}$$

and the restricted sumsets

$$h\hat{\ }A = \{a_{j_1} + \cdots + a_{j_h} : a_{j_i} \in A \ \forall i = 1, \ldots, h, a_{j_x} \neq a_{j_y} \text{ for } x \neq y\}$$

can be recovered from this notation, since $hA = h^{(h)}A$ and $h\hat{\ }A = h^{(1)}A$.

When $G = \mathbb{Z}$ lower bounds for the cardinality of sumsets and restricted sumsets are well-known.

In this setting, the problem of giving lower bounds for the cardinality of $h^{(r)}A$ for nontrivial values of h, r and k has been studied in [1], where the authors proved the following theorem holding for subsets of the integers.

Theorem 1.1. *Let h, r be non-negative integers, $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$. Let A be a nonempty finite set of integers with $|A| = k$ such that $1 \leq h \leq rk$. Then*

$$|h^{(r)}A| \geq hk - m^2 r + 1 - 2m\epsilon - \epsilon. \tag{1}$$

Here the condition $h \leq rk$ is necessary, for otherwise the set $h^{(r)}A$ would be empty.

The lower bound in Theorem 1.1 is the best one possible, as shown by any arithmetic progression.

A generalization of theorem 1.1 can be found in [2], where the authors proved lower bounds for generalized sumsets where the jth element of A can be repeated up to r_j times, with the r_j's not necessarily all equal to r.

In the first section of this paper we will exhibit a new proof of theorem 1.1

In the second section we prove the main result of the paper, which states that a similar lower bound also holds when $G = \mathbb{Z}/p\mathbb{Z}$ for a prime p.

Theorem 1.2. *Let $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$. Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a nonempty set with $|A| = k$ such that $1 \leq r \leq h \leq rk$. Then*

$$|h^{(r)}A| \geq \min(p, hk - m^2 r + 1 - 2m\epsilon - \epsilon).$$

The authors in [1] also solved the inverse problem related to $h^{(r)}A$, showing that, up to a few exceptions, any set A satisfying (1) must be an arithmetic progression:

Theorem 1.3. *Let $k \geq 5$. Let r and $h = mr + \epsilon, 0 \leq \epsilon \leq r - 1$ be integers with $2 \leq r \leq h \leq rk - 2$. Then any set of k integers A such that*

$$|h^{(r)}A| = hk - m^2 r + 1 - 2m\epsilon - \epsilon \tag{2}$$

2

is a k-term arithmetic progression.

In the third section we show how we can deduce Theorem 1.3 from the results in the first two sections and discuss the analogue problem in groups of prime order.

2. Direct problem

To prove Theorem 1.1, and later Theorem 1.2, we first deal with the case $r|h$, showing that for a subset A of an abelian group G we have $h^{(r)}A = r(m\hat{\ }A)$.

Lemma 2.1. *If $h = mr$, $A \subseteq G$, $|A| = k$ and $rk \geq h \geq 1$, then*

$$h^{(r)}A = r(m\hat{\ }A).$$

Proof. Clearly $r(m\hat{\ }A) \subseteq h^{(r)}A$, since no element in A can be summed more than r times in order to get an element of $r(m\hat{\ }A)$.

To prove the converse inclusion, take $x \in h^{(r)}A$ so that, after reordering the elements of A if necessary, $x = \sum_{i=1}^{l} r_i^{(0)} a_i$ with $1 \leq l \leq k, 1 \leq r_i^{(0)} \leq r$ and $\sum_{i=1}^{l} r_i^{(0)} = h$. Let also $r_i^{(0)} = 0$ for $l+1 \leq i \leq k$.

We now describe an algorithm which shows how we can write x as an element in $r(m\hat{\ }A)$.

If possible, for every $j = 1, \ldots, r$ take distinct elements $r_{j_1}^{(j-1)}, \ldots, r_{j_m}^{(j-1)}$ which are greater or equal to the remaining $r_s^{(j-1)}$ and define

$$x_j = \sum_{i=1}^{m} a_{j_i},$$

$$r_s^{(j)} = \begin{cases} r_s^{(j-1)} - 1 & \text{if } s = j_i \text{ for some } i = 1, \ldots, m \\ r_s^{(j-1)} & \text{otherwise.} \end{cases} \quad (3)$$

If we can apply this pocedure for every $j = 1, \ldots, r$, then we can write $x = x_1 + \cdots + x_r$ with $x_i \in m\hat{\ }A$, thus proving $h^{(r)}A \subseteq r(m\hat{\ }A)$.

To do this we need to prove that at every step $j = 1, \ldots, r$ the following two conditions are satisfied:

3

1. $|\{r_i^{(j-1)} \geq 1\}_i| \geq m$,

2. $\max_{1 \leq i \leq k}(r_i^{(j)}) \leq r - j$.

Since $\sum_{i=1}^{k} r_i^{(0)} = h = mr$, the first condition holds for $j = 1$, and so we can define $r_i^{(1)}$ as in (3). Clearly $\max_i(r_i^{(1)}) \leq r - 1$, for otherwise we could find $m + 1$ distinct indexes s such that $r_s^{(0)} = r$, which would imply $\sum_{i=1}^{k} r_i^{(0)} \geq (m + 1)r > h$, a contradiction.

Suppose now that condition (1) does not hold for every $j \in [1, r]$, and let j' be the minimal j such that

$$|\{r_i^{(j'-1)} \geq 1\}| = N < m.$$

By what observed above we must have $2 \leq j' \leq r$.

We have

$$r_i^{(j'-2)} \begin{cases} > 1 & \text{for } a \text{ indexes, } a \leq N < m \\ = 1 & \text{for } b \text{ indexes} \\ = 0 & \text{for all the remaining } k - a - b \text{ indexes,} \end{cases}$$

so that $N = a + b - (m - a) = 2a + b - m$.

By the minimality of j' we also have that $a + b \geq m$.

Next we show that condition (2) holds for all $0 \leq j'' \leq j' - 2 \leq r - 2$.

In fact, if this does not happen, take the minimal $j'' \leq j' - 2$ which fails to satisfy condition (2), i.e.

$$\max_{1 \leq i \leq k}(r_i^{(j'')}) \geq r - j'' + 1.$$

By the minimality of j'' we must have that $r_i^{(j''-1)} = r - (j'' - 1)$ for at least $m + 1$ values of i, because of how the $r_i^{(j)}$ are recursively defined in (3).

This implies that

$$h - m(j'' - 1) = \sum_{i=1}^{k} r_i^{(j''-1)} \geq (m + 1)(r - j'' + 1) = h - m(j'' - 1) + r - j'' + 1,$$

a contradiction since $r \geq j''$.

Hence we have that for all $0 \leq j'' \leq j' - 2$ condition (2) is satisfied, which means $\max_i(r_i^{(j'')}) \leq r - j''$.

In particular, since $2a + b = N + m < 2m$ and $a < m$, we get

$$h - m(j' - 2) = \sum_{i=1}^{k} r_i^{(j'-2)}$$
$$\leq a(r - (j' - 2)) + b$$
$$< m(r - j') + 2m$$
$$= h - m(j' - 2),$$

a contradiction.

Hence conditions (1) and (2) are satisfied for all $j = 1, \ldots, r$. $\qquad\square$

Before proving Theorem 1.1, recall the following well-known results on the cardinality of sumsets and restricted sumsets.

Theorem 2.1. *[3, Theorem 1.3] Let $h \geq 2$. Let A be a nonempty finite set of integers with $|A| = k$. Then*

$$|hA| \geq hk - h + 1.$$

Theorem 2.2. *[3, Theorem 1.9] Let $h \geq 2$. Let A be a nonempty finite set of integers with $|A| = k$. Then*

$$|h\hat{\,}A| = hk - h^2 + 1$$

Proof of Theorem 1.1. Let $A = \{a_1 < a_2 < \cdots < a_k\}$.

The case $\epsilon = 0$ is covered by Lemma 2.1, since the claim follows from the lower bounds for sumsets and restricted sumsets.

From now on, assume $\epsilon \geq 1$.

From the condition $rk \geq h = mr + \epsilon$ we get $k \geq m + 1$.

We split the proof in two cases.

Case 1. $m + \epsilon \leq k$.

In this case it's easy to see the inclusion

$$B := (r - 1)(m\hat{\,}A) + (m + \epsilon)\hat{\,}A \subseteq h^{(r)}A,$$

5

where both the summands are nonempty and $h = (r-1)m + m - \epsilon$.

Then, by Theorems 2.1 and 2.2 we have

$$
\begin{aligned}
|h^{(r)}A| &= |B \coprod (h^{(r)}A \setminus B)| \\
&\geq hk - m^2r + 1 - 2m\epsilon - \epsilon^2 + |h^{(r)}A \setminus B|. \tag{4}
\end{aligned}
$$

We can now estimate the cardinality of the remaining set observing that

$$
\min A = r \sum_{i=1}^{m} a_i + \epsilon a_{m+1},
$$

$$
\min B = r \sum_{i=1}^{m} a_i + \sum_{i=m+1}^{m+\epsilon} a_i.
$$

If we let

$$
S_{x,y} = r \sum_{i=1}^{m} a_i + \sum_{i=1}^{x} a_{m+i} + y a_{m+x} + (\epsilon - x - y)a_{m+x+1},
$$

with $x \in [1, \epsilon - 1], y \in [0, \epsilon - x]$, we have $S_{x,y} \in h^{(r)}A$, and

$$
\begin{aligned}
S_{1,\epsilon-1} \quad &< S_{1,\epsilon-2} \quad < S_{1,\epsilon-3} \quad < \ldots \quad < S_{1,0} \\
&< S_{2,\epsilon-3} \quad < S_{2,\epsilon-4} \quad < \ldots \quad < S_{2,0} \\
&\qquad \ldots \\
&\qquad\qquad\qquad < S_{\epsilon-2,1} \quad < S_{\epsilon-2,0} \\
&\qquad\qquad\qquad\qquad\qquad < S_{\epsilon-1,0}.
\end{aligned}
$$

Moreover, all these elements, except for $S_{\epsilon,0}$ are in $[\min A, \min B - 1]$, which gives

$$
|(h^{(r)}A \setminus B) \cap [\min A, \min B - 1]| \geq \sum_{i=1}^{\epsilon-1} i = \frac{\epsilon^2 - \epsilon}{2}.
$$

A symmetric argument gives

$$
|(h^{(r)}A \setminus B) \cap [\max B + 1, \max A]| \geq \sum_{i=1}^{\epsilon-1} i = \frac{\epsilon^2 - \epsilon}{2}.
$$

This, combined with equation (4), gives the desired lower bound for $|h^{(r)}A|$.

Case 2: $m + \epsilon > k$.

As already observed in [1], we have $|h^{(r)}A| = |(rk - h)^{(r)}A|$.

6

Then, if $r - 1 \leq m + \epsilon$,

$$|h^{(r)}A| = |(r(k - m - 1) + (r - \epsilon))^{(r)}A|,$$

and hence we can argue as in the first case to obtain the desired lower bound.

Suppose now $r - 1 > m + \epsilon > k$. Then

$$B = (m + \epsilon)((m + 1)\hat{}A) + (r - 1 - m - \epsilon)(m\hat{}A) \subseteq h^{(r)}A$$

and again

$$
\begin{aligned}
|h^{(r)}A| &= |B \coprod (h^{(r)}A \setminus B)| \\
&\geq hk - m^2 r + 1 - 2m\epsilon - \epsilon - (m^2 + m) + |h^{(r)}A \setminus B|. \qquad (5)
\end{aligned}
$$

Observe that

$$
\begin{aligned}
\min B &= (m + \epsilon) \sum_{i=1}^{m+1} a_i + (r - 1 - m - \epsilon) \sum_{i=1}^{m} a_i \\
&= (r - 1) \sum_{i=1}^{m} a_i + (m + \epsilon)a_{m+1}, \\
\min A &= r \sum_{i=1}^{m} a_i + \epsilon a_{m+1}.
\end{aligned}
$$

If we let

$$T_{x,y} = (r - 1) \sum_{i=1}^{m} a_i + \epsilon a_{m+1} + \sum_{i=x, i \neq y}^{m} a_i + x a_{m+1},$$

with $x \in [1, m], y \in [x, m]$, we have $T_{x,y} \in h^{(r)}A$, and

$$
\begin{aligned}
\min A \;&< T_{1,m} \;< T_{1,m-1} \;< \ldots \;&< T_{1,1} \\
&< T_{2,m} \;< T_{2,m-1} \;< \ldots \;&< T_{2,2} \\
&\qquad \ldots & \\
&&< T_{m-1,m} \;< T_{m-1,m-1} \\
&&< T_{m,m}.
\end{aligned}
$$

All these elements but $T_{m,m}$ belong to $[\min A, \min B - 1]$, which implies

$$|(h^{(r)}A \setminus B) \cap [\min A, \min B - 1]| \geq \sum_{i=1}^{m} i = \frac{m^2 + m}{2}.$$

7

A symmetric argument gives

$$|(h^{(r)}A \setminus B) \cap [\max B + 1, \max A]| \geq \sum_{i=1}^{m} i = \frac{m^2 + m}{2},$$

thus leading, combined with (5), to the desired lower bound. $\square$

3. Direct problem in groups of prime order

In order to prove Theorem 1.2 we need the analogues of Theorems 2.1 and 2.2 in $\mathbb{Z}/p\mathbb{Z}$.

Theorem 3.1 (Cauchy-Davenport). *Let $h \geq 1$. Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a nonempty set of residues modulo a prime p with $|A| = k$. Then*

$$|hA| \geq \min(p, hk - h + 1).$$

Theorem 3.2 (Erdős-Heilbronn). *Let $h \geq 1$. Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be a nonempty set of residues modulo a prime p with $|A| = k$. Then*

$$|h\hat{\ }A| \geq \min(p, hk - h^2 + 1).$$

Theorem 3.2 was conjectured by Erdős and Heilbronn and proved in [4] by Da Silva and Hamidoune and later, using the polynomial method, in [5] by Alon, Nathanson and Ruzsa.

Proof of Theorem 1.2. The proof goes by induction on ϵ.

If $\epsilon = 0$, thanks to Lemma 2.1 and Theorems 3.1 and 3.2, we have:

$$
\begin{aligned}
|h^{(r)}A| &= |r(m\hat{\ }A)| \geq \min(p, r|m\hat{\ }A| - r + 1) \\
&\geq \min(p, r\min(p, mk - m^2 + 1)) - r + 1) \\
&= \min(p, hk - rm^2 + 1),
\end{aligned}
$$

where the last equality follows since if $p \leq mk - m^2 + 1$ then, for $r \geq 1$, $p \leq hk - rm^2 + 1$.

Let now $\epsilon \in [1, r - 1]$.

From $rk \geq h = mr + \epsilon$ we get $k \geq m+1$, and so $h - m - 1 = m(r-1) + \epsilon - 1 = m(r-1) + \epsilon' \leq (m+1)(r-1) \leq k(r-1)$.

We then have the following inclusion

$$(m+1)\hat{}A + (h-m-1)^{(r-1)}A \subseteq h^{(r)}A, \tag{6}$$

where both summands are nonempty because of the inequalities above.

Moreover, $\epsilon' \in [0, r-2], \epsilon' < \epsilon$ and so, by the inductive hypothesis and Theorems 3.1 and 3.2 we have

$$
\begin{aligned}
|h^{(r)}A| &\geq |(m+1)\hat{}A + (h-m-1)^{(r-1)}A| \\
&\geq \min(p, |(m+1)\hat{}A| + |(h-m-1)^{(r-1)}A| - 1) \\
&= \min(p, hk - m^2r - 2m\epsilon - \epsilon + 1). \tag{7}
\end{aligned}
$$

$\square$

Since the inclusion (6) holds in any group, our proof, with the obvious modifications, still holds in any abelian group in which theorems similar to 3.1 and 3.2 hold. See [6] for an extensive treatment of the subject.

In particular, when adapted to $\mathbb{Z}$, this leads to yet another proof of Theorem 1.1.

4. Inverse problem

From our proof of Theorem 1.1 it's easy to deduce the inverse theorem based on the well-known results for sumsets and restricted sumsets:

Theorem 4.1. *[3, Theorem 1.5] Let $h \geq 2$. Let $A_1, A_2, \ldots, A_h$ be h nonempty finite sets of integers. Then*

$$|A_1 + \cdots + A_h| = |A_1| + \cdots + |A_h| - h + 1$$

if and only if the sets $A_1, \ldots, A_h$ are arithmetic progressions with the same common difference.

9

Theorem 4.2. *[3, Theorem 1.10] Let $h \geq 2$. Let A be a nonempty finite set of integers with $|A| = k \geq 5$, $2 \leq h \leq k - 2$. Then*

$$|h\hat{\,}A| = hk - h^2 + 1$$

if and only if A is a k-term arithmetic progression.

Proof of Theorem 1.3. First of all observe that the hypothesis on h, r and k imply that $m \leq k - 1$.

Consider first the case $r | h$.

If $m = 1$, then $h^{(r)}A = r^{(r)}A = rA$, and Theorem 4.1 can be applied to obtain the thesis.

Let $m \geq 2$. Since $\epsilon = 0$, by Lemma 2.1 we have

$$h(k - m) + 1 = |h^{(r)}A| = |r(m\hat{\,}A)| \geq r|m\hat{\,}A| - r + 1 \geq h(k - m) + 1.$$

Hence all inequalities above are actually equalities.

In particular, by Theorem 4.1, $m\hat{\,}A$ must be an arithmetic progression.

If $m = k - 1$, then

$$(k-1)\hat{\,}A = \left\{ \left(\sum_{i=1}^{k} a_i \right) - a_k < \left(\sum_{i=1}^{k} a_i \right) - a_{k-1} < \ldots \left(\sum_{i=1}^{k} a_i \right) - a_1 \right\}, \quad (8)$$

and clearly this set is an arithmetic progression if and only if A is an arithmetic progression too.

If $2 \leq m \leq k - 2$ we can apply Theorem 4.2 to get the thesis.

Let now $h = mr + \epsilon, \epsilon \in [1, r - 1]$.

For $m = 0$ we have $h^{(r)}A = \epsilon^{(r)}A = \epsilon A$, and Theorem 4.1 is enough to finish the proof.

Recalling that $(m + 1)\hat{\,}A + (h - m - 1)^{(r-1)}A \subseteq h^{(r)}A$, from the equation (2) we deduce that

$$|(m + 1)\hat{\,}A| = (m + 1)k - (m + 1)^2 + 1 \qquad (9)$$

and

$$|(h - m - 1)^{(r-1)}A| = (h - m - 1)k - m^2(r - 1) + 1 - 2m(\epsilon - 1) - \epsilon + 1. \quad (10)$$

10

By Theorem 4.2 we get the desired conclusion from (9) if $2 \leq m+1 \leq k-2$.

Since we already know that $m + 1 \leq k$, only the cases $m = k - 2$ and $m = k - 1$ are left to study.

If $m = k - 2$, then $(m + 1)\hat{}A = (k - 1)\hat{}A$ and, since (8) holds, we get the thesis.

If $m = k - 1$, then $(h - m - 1)^{(r-1)}A = (h - k)^{(r-1)}$, and

$$|(h - k)^{(r-1)}A| = |[(r - 1)k - h + k]^{(r-1)}A| = |(r - \epsilon)^{(r-1)}A| = |(r - \epsilon)A|$$

since $r - \epsilon \in [1, r - 1]$.

This, combined with equation (10) and Theorem 4.1, gives the desired conclusion.

□

As far as the inverse problem modulo a prime is concerned, in [7] the inverse theorem of the Erdős-Heilbronn conjecture is proved.

Theorem 4.3. *Let A be a set of residue classes modulo a prime p with $|A| = k \geq 5, p > 2k - 3$. Then*

$$|2\hat{}A| = 2k - 3$$

if and only if A is a k-term arithmetic progression.

The proof however works only when adding two copies of A and, to the best of the author's knowledge, an inverse theorem for $h\hat{}A$, $h > 2$, does not exist yet.

Clearly, an inverse theorem for $h^{(r)}A$ would imply such a result. However, the inclusion (6) shows that the converse also holds, showing that the two inverse problems are actually equivalent.

References

References

[1] R. Mistri, R. Pandey, A generalization of sumsets of set of integers, J. Number Theory 143 (2014) 334–356.

[2] Q.-H. Yang, Y.-G. Chen, On the cardinality of general h-fold sumsets, European J. Combin. 47 (2015) 103–114.

[3] M. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, 1996.

[4] J. A. D. da Silva, Y. O. Hamidoune, Cyclic spaces for grassmann derivatives and additive theory, Bull. Lond. Math. Soc. 26 (1994) 140–146.

[5] N. Alon, M. Nathanson, I. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56 (2) (1996) 118–173.

[6] G. Károly, The Erdős-Heilbronn problem in abelian groups, Israel J. Math. 139 (2004) 349–359.

[7] G. Károly, An inverse theorem for the restricted set addition in abelian groups, J. Algebra 290 (2005) 557–593.